Serial No.: 10/713,481

REMARKS

Claims 1-18 are pending in the application. Claims 1, 3, 5, 7, 8, 10, 12, 14, 16 and 17. Claims 2, 4, 9, 11, 13, and 18 have been canceled. Favorable reconsideration of the application, as amended, is respectfully requested.

I   AMENDMENTS TO THE DRAWINGS AND SPECIFICATON.

Amendments have been made to Figure 1 to add reference numerals to two elements referenced in the specification and shown on the drawings. No new matter has been added.

Amendments to the specification have been made to correct reference numerals. No new matter has been added.

II   REJECTION OF CLAIMS UNDER 35 USC 35 USC § 103

Claims 1-18 stand rejected under 35 USC 103(a) as being unpatentable over US Patent 6,519,635 to Champlin and US Patent 5,991,806 to McHann in view of US Patent 7,225,249 to Barry.

General Discussion of Applicant's invention

The Simple Network Management Protocol (SNMP) is a well known communication protocol that enable an SNMP Manager (also known as an SNMP Managing System) to collect data from SNMP managed clients (also known as SNMP managed systems or agents).

It is well known that SNMP utilizes UDP/IP messaging to predefined ports and, as such, an SNMP request can not be sent from an SNMP Manager on the Internet "inbound" to an SNMP managed client that is on a local area network served by a NAT firewall (e.g. a network utilizing the subset of IP addresses reserved for local area networks).

In a NAT firewall environment message exchanges can only be initiated by the client device on the local network and responded to by the device on the Internet.

11

Serial No.: 10/713,481

With reference to the applicant's Figure 1, the applicant's invention is to a novel sub manager system 20. The sub manager 20 operates, with respect to an SNMP Managing System 22, as an SNMP managed client exchanging SNMP messages in the ordinary course. The sub manager operates, with respect to each SNMP managed client 18, as an SNMP manager – but with the exception that messaging is sent utilizing a connection maintained through the firewall.

A novel sub manager and method for generating SNMP messes to a managed client in response to receipt of a request message is disclosed. In more detail, the SNMP manager 22 sends a master SNMP network management request message to the Sub Manager. The Sub Manager generates and sends SNMP network management requests to each of the clients, each through the connection maintained with such client through the firewall.

A response is received from each client. The responses are aggregated into a single response message back to the SNMP Manager 22.

Claim 1

With reference to Figure 1, the applicant's invention, as defined in claim 1, is to a sub manager 20 for interfacing between an SNMP network management system 22 and a plurality of SNMP managed clients 18. Each of such SNMP managed clients 18a, 18b, 18c is served by a network address translation firewall 16a, 16b.

The sub-manager 20 comprises a network management agent 25. The network management agent: i) receives a master SNMP network management request message 170 (Figure 6 and Figure 8) from the SNMP network management system 22; and ii) provides a master SNMP response message 192 (Figure 6 and Figure 8) to the SNMP network management system (See Page 14, Lines 6-15).

With reference to Figure 6, the master SNMP network management request message 170 includes a plurality of variable values 176. Each variable value 176 is identified by a master object identifier 182 selected from within a master

12

Serial No.: 10/713,481

information base 32. (Figure 6, Page 18, Lines 2-9). With reference to Figure 1, each master object identifier 182 comprises:

    i)   a client identifier 46 that identifies a particular one of the plurality of SNMP managed clients 18 which has a client management information base 34 that includes the variable value (reference number 44 in the client management information base 34); and

    ii)   a variable identification portion 210, the variable identification portion 210 being a client object identifier 188 that identifies the variable value 44 within the client management information base 34. (Page 20, Lines 5-11)

        With respect to these elements, the examiner, cites Champlin's network management agent (block 64, Figure 4) as teaching applicant's connections module 24 receiving a master SNMP request message and providing a master SNMP response. The examiner cites Champlin's SNMP PDU (Figure 3, Block 40) as teaching the applicants master SNMP request message.

        Champlin describes a format of the PDU at C2, L58 to C3, L2 and indicates its format is illustrated in Figure 3. More specifically, Champlin indicates that PDU includes the address of the object to be controlled, a desired command (e.g. Set or Get), and an appropriate value.

        Even if it taken that the "appropriate value" of the Champlin PDU is comparable to each variable value 176 of the applicant's master SNMP management request message 170 and, even if it is taken that Champlin's header or address is comparable to applicant's client identifier 46 of the master object identifier 182, Champlin still fails to teach a client object identifier 188 as a portion of the master object identifier 183 (in addition to the client ID) that identifies the variable value within the client management information base 34.

        As additional claim elements, the sub-manager 20 further comprises a

13

Serial No.: 10/713,481

connections module 24. The connections module 24, for each of the plurality of
SNMP managed clients 18a, 18b, 18c, establishes an internet protocol connection
45 with such SNMP managed client 18 through the firewall 16 serving such SNMP
managed client 18. (See Page 15, Lines 15-16 and Page 4, Line 30 to Page 5,
Line 2)

Through the internet protocol connection 45, the connections module 24
both: i) provides, to each of the plurality of SNMP managed clients 18, a client
network management request message 172 (Figure 6, Figure 4b, step 125, Page
17, Lines 14-15); and ii) receiving, from each of the plurality of SNMP managed
clients 18, a client response message 206 (Figure 7, Figure 4b, Step 127, Page 16,
Lines 13-14, Page 16, Lines 25-26).

With respect to these elements, the examiner, references Champlin
C2, Line 58 through C3, line 14 and C4, Lines 49-64 as teaching the
applicant's connection module and its recited functions for establishing
internet protocol connections with SNMP managed clients.

First, the applicant respectfully disagrees with the examiners
conclusion that Champlin teaches the applicant's connection module and its
recited functions for establishing internet protocol connections with SNMP
managed clients. It should be noted that Champlin never uses the term
"internet connection protocol" and does not include teaching that Champlin's
SNMP messaging is anything other than traditional SNMP messaging with is
known to those skilled in the art to be a connection-less protocol (e.g. it
utilizes UDP/IP – not TCP/IP). Therefore, based on the field of art, the
distinction between an internet protocol connection and connection-less
protocol messaging (which still uses an IP header) is critical. In view of the
principal objective of the applicant's invention being a system for SNMP
messaging utilizing an internet protocol connection through a firewall (where
traditional SNMP utilizing a connection-less protocol would not work), the
applicant disagrees with the examiner's assertion that Champlin teaches

14

Serial No.: 10/713,481

establishing internet protocol connections with SNMP managed clients – when in fact it does not teach internet protocol connections.

Further, it is noted that McHann indicates at C1, L30-33 that SNMP is developed for usage in a TCP/IP community. The applicant acknowledges that SNMP messaging is often used in an IP network that operates both TCP/IP connection protocols and UDP/IP connection-less messaging. McHann does not include any enabling teaching of use TCP/IP for SNMP messaging – and specifically does not include the applicants claimed invention for effecting SNMP management utilizing TCP/IP connections for firewall penetration.

As the examiner has acknowledged in both the first office action and the second office action, neither Champlin nor McHann teach establishing an internet protocol connection through a firewall serving the SNMP managed client. Both references being silent on operation of SNMP messaging through firewalls would be expected by those skilled in the art because SNMP messages (which utilizes UDP/IP) can not be sent inbound through a network address translation (NAT) firewall unless a "permanent hole" is established through the NAT firewall (see the background of the applicant's invent). The examiner references Barry as teaching TCP/IP connections which may be established through a NAT firewall.

As discussed, one of the objectives of the applicant's invention is to provide a novel structure and method to specifically provide for SNMP management of clients which are behind a NAT firewall and therefore are unable to be services by connection-less UDP/IP messaging (see the background of the applicant's specification).

Neither Champlin nor McHann even teach or suggest NAT firewall penetration with SNMP messaging. Further, even in combination Barry, the applicant's specific sub-manager, as claimed, for SNMP management of clients behind NAT firewalls is not taught.

15

Serial No.: 10/713,481

As yet additional elements, the sub-manager 20 further comprises a message handling module 26. With reference to Figure 6 and Figure 9a and page 15, lines 5-19, the message handling module 26 performs at least the three following steps:

1.   Receives the master SNMP network management request message 170;

2.   For each master object identifier 182 included in the master SNMP network management request message 170, generates the client network management request message 172 (Page 20, Lines 22-24). Each client network management request message 172 includes the client object identifier 188 that identifies the variable value 44 within the client management information base 34 (Figures 1 and 6, Page 4, Lines 22-23); and

3.   Generates the master SNMP response message 192 from each received client response message 206, wherein:

Each client response message 206 includes the client object identifier 188 and the variable value (Figures 1 and 6, Page 4, Lines 25-26); and

The master SNMP response message 192 includes each of the master object identifiers 182, and each of the master object identifiers 182 is associated with the variable value 176 received in the client response message 206 (Figure 6, Page 4, Lines 26-29 and Page 20, Line 19 to Page 21, Line 13)

With respect to these elements, the examiner cites Champlin C2, Line 58 – C3, L14 and C4, L49-64 as: i) teaching generating the client network management request message for each master object identifier included in the master SNMP network management message; and ii) teaching a client network management request message including a client object identifier that identifies the variable value within the client management information base.

The applicant's invention specifically cites that the client management request message 172 includes the client object identifier 188 that identifies

16

Serial No.: 10/713,481

the variable value 44 within the client management information base 34 –
noting that the antecedent basis for the client object identifier is within the
variable identification portion of the master object identifier of the master
network management request message.

In one aspect, Champlin teaches "reformatting an SNP PDU to a
format which can be recognized by an associates SNMP sub-agent" (C3,
L9-11). In another aspect, Champlin teaches a translation table 70 which
apparently provide direct translation between MIB object identifies and
database record protocols.

In neither aspect does Champlin teach the applicant's novel system
and method for generating client network management request messages
from a master network management request message that comprises: i)
inclusion of the client object identifier within the variable identification portion
of the master object identifier of the master network management request
message; and ii) use of such client object identifier for the client network
management request message.

For at least these reasons, the applicant respectfully asserts that Claim 1 is
allowable over Champlin, Barry, McHann, and the other art of record.

Claim 7

Claim 7, which depends from claim 1 and has not been substantively
amended, further specifies that the master SNMP network management request
message comprises at least two master object identifiers, each master object
identifier comprising a client identifier that is unique from the client identifier of at
least one other master object identifier.

As discussed, with respect to Claim 1, each master object identifier 182
comprises:

  i) a client identifier 46 that identifies a particular one of the plurality of
SNMP managed clients 18 which has a client management information base 34

17

Serial No.: 10/713,481

that includes the variable value (reference number 44 in the client management information base 34); and

ii)   a variable identification portion 210, the variable identification portion 210 being a client object identifier 188 that identifies the variable value 44 within the client management information base 34. (Page 20, Lines 5-11)

As discussed with respect to claim 1, even if it taken that the "appropriate value" of the Champlin PDU is comparable to each variable value 176 of the applicant's master SNMP management request message 170 and, even if it is taken that Champlin's header 42 or address 48 is comparable to applicant's client identifier 46 of the master object identifier 182, Champlin still fails to teach a client object identifier 188 as a portion of the master object identifier 183 (in addition to the client ID) that identifies the variable value within the client management information base 34. Further, with respect to applicants claim limitation that the SNMP network management request message 170 includes at least two such master object identifiers 188, each master object identifier 188 comprising a client identifier that is unique from the client identifier of at least one other master object identifier 188, Champlin fails to teach, suggest, or in any way enable a PDU with headers 42 or two addresses 48 unique from each other.

For at least these reasons, in addition to the reasons described with respect to independent claim 1, the applicant respectfully asserts that Claim 7 is allowable over Champlin, Barry, McHann, and the other art of record.

Claim 3

Claim 3, as amended and depending from claim 7, further specifies that each internet protocol connection 45 is a TCP/IP connection that is established with the SNMP managed client 18, through the firewall 16 serving such SNMP managed client in response to receiving a connection request initiating by such SNMP managed client (Figure 4a, step 116 and Page 15, 17-19).

18

Serial No.: 10/713,481

The connections module 24 further records, in response to receiving an SNMP inform message from the SNMP managed client 18 through the internet protocol connection 45, the SNMP inform message including the SNMP managed client's client identifier 46:

    1)   spawns a device state machine for the SNMP managed client (Page 15, Lines 23-28); and

    2)   records in an active connections table 28 and in association with the client identifier 46:

        i)   a client connection identifier 48, the client connection identifier comprising the source IP address 50 and source port number 52 of the SNMP inform message initiated by the SNMP managed client and translated by the firewall serving the client; and

        ii)   a device state machine identifier identifying the device state machine (Figure 1, Figure 4a, and Page 15, Line 29 to Page 16, Line 7); and

the device state machine provides the client network management request message to the SNMP managed client by providing the client network management request message over the internet protocol connection that associates, in the active connections table, with the client identifier of the master object identifier (Figure 1, Page 17, Line 11-16 –- plus bring in some from original claim).

With respect to these elements, the examiner cites Champlin C2, L58 through C3, line 14 and C4, L49-64 as disclosing each internet protocol connection being established with an SNMP managed client, recording, in an active connections table, for each internet protocol connection, a client connection identifier in association

The application respectfully disagrees with the assertion that Champlin teaches such elements. Champlin fails to teach recording, in the active connections table 28, in association with the SNMP managed client's client identifier 46: i) a client connection identifier 48 that comprises the source IP address 50 and source port number 52 of the SNMP inform

19

Serial No.: 10/713,481

message initiated by the SNMP managed client and translated by the firewall serving the client; and ii) a device state machine identifier 49 identifying the device state machine spawned for serving the SNMP managed client.

Further, the examiner cites McHann C1, lines 27-37, C8L56 to C9, L1 as teaching the <u>client identifier</u> is a source IP address and a source port number obtained form a TCP/IP frame initiated by the SNMP managed client.

In the applicants claim, the SNMP managed client's <u>client identifier 46</u> is associated, in the active connections table 28 the with <u>a client connection identifier 48</u> that comprises the source IP address 50 and source port number 52 of the SNMP inform message initiated by the SNMP managed client 18 and translated by the firewall 16 serving the client 18. Such structure is not taught by McHann, Champlin, nor Barry.

For at least these reasons, in addition to the reasons described with respect to independent claim 1 and intervening claim 7, the applicant respectfully asserts that Claim 3 is allowable over Champlin, Barry, McHann, and the other art of record.

Claim 5

Claim 5, which has been amended to depend from claim 7 but not otherwise substantively amended, further defines the device state machine as providing for:

periodically receiving a heart beat message from the SNMP managed client over the internet protocol connection; each heart beat message including the client identifier and a time interval between the heart beat message and a subsequent heart beat message;

updating the client connection identifier in the active connection table if the source IP address or the source port number obtained from the heart beat message differs from that of a previous heart beat message;

20

Serial No.: 10/713,481

providing a heart beat acknowledgement message to the SNMP managed
client over the internet protocol connection; and

determining that the internet protocol connection is inactive if a time period
in excess of the time interval elapses during which a subsequent heart beat
message has not been received.

With respect to these elements, the examiner generally cites McHann
C10, Line 34 to C11, Line 60 as teaching: i) receipt of a heart beat message
including the client identifier; ii) updating the client connection identifier in
the active connections table if the source IP address or the source port
number obtained form the heart beat message differs from a previous heart
beat messaging and providing a heart beat acknowledgement to the SNMP
managed client.

The applicant respectfully disagrees. McHann Figures 4 and 5
depict a well known SNMP architecture wherein a Managing System 402
(Figure 4, 502 in Figure 5) utilizes SNMP management protocols to
communicate with one or more Agents 412 of the Managed Systems (404 in
Figure 4, 504 in Figure 5). As is well known in the art of network
management, the SNMP management protocols utilize UDP/IP messaging
over an IP compliant network.

With reference to Figure 1, McHann teaches a message router 104
which executes on a computer system 102 and determines local computer
system events such as (ACPI, SMI, PnP, DMI, an OS events) and generates
messages in a common format that may be sent over a network 104. SNMP
is a representative common format.

In more detail, McHann teaches a software application (Dynamic
System Control 810 as depicted in Figure 8) which resides on one of the
managed systems. The DSC 810 monitors local events on the system bus
(such as DMI, SMI, OS or other system messages) and generates common
format messages (e.g. SNMP messages) to the Managing System over the

21

Serial No.: 10/713,481

IP network 802 (note, network 802 is near the bottom of McHann Figure 8, it is unknown why the processor is also labeled 802).

The DSC 810 monitors the system bus to detect such "lower level" local events or otherwise receives such local events – and passes common format (e.g. SNMP messages) up to the SNMP Managing System. The system components are not SNMP managed clients and there is no teaching in McHann of requesting information from any of the system components.

With specific respect to McHann's teachings of signaling at C10, Line 34 to C11, Line 60, the applicant asserts that such signaling across a system bus internal to the computer system (202 in Figure 2, unlabeled in Figure 8) which specifically is not SNMP messaging – and there is no internet protocol signaling across the system bus, no IP addressing across the system bus, nor are source port number usage.

McHann utilizes the term "network" interchangeably to refer to both the system bus and the IP network 100 (Figure 1) – with are entirely different structures with entirely different functions. Such unorthodox and interchangeable use of the term "network" does not in any way teach, suggest, nor enable SNMP signaling (which occurs on the IP network 100 of McHann) on the system bus – nor does such interchangeable use of language teach or suggest that SNMP signaling is interchangeable with the local computer system event signals sent over the system bus 202.

For this reason, the applicant respectfully traverses the examiners position that local computer system events sent over the system bus 202 as described at C10, Line 34 to C11, Line 60 teaches or suggests the applicant's invention as described in Claim 5.

For at least these reasons, in addition to the reasons described with respect to independent claim 1 and intervening claims 7 and 3, the applicant respectfully

22

Serial No.: 10/713,481

asserts that Claim 5 is allowable over Champlin, Barry, McHann, and the other art of record.

Claim 6

Claim 6 depends from claim 6 and is distinguishable over Champlin, McHann, and Barry for at least the reasons described with respect to independent claim 1 and intervening claims 7, 3, and 5.

Claim 8

Claim 8 depends from claim 7 and is distinguishable over Champlin, McHann, and Barry for at least the reasons described with respect to independent claim 1 and intervening claim 7.

Claims 10, 12, and 14-17

As the examiner has indicated, claims 10, 12, and 14-17 are method claims of claims 1, 3, and 5-8 respectively. Claims 10, 12, and 14-17 are therefore distinguishable over Champlin, McHann, and Barry for at least the same reasons as discussed with respect to claims 1, 3, and 5-8.
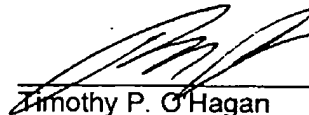
III.   CONCLUSION

Accordingly, Claims 1, 3, 5-8, 10, 12, and 14-17 are believed to be allowable and the application is believed to be in condition for allowance. A prompt action to such end is earnestly solicited.

Should the Examiner feel that a telephone interview would be helpful to facilitate favorable prosecution of the above-identified application, the Examiner is invited to contact the undersigned at the telephone number provided below.

Serial No.: 10/713,481

Respectfully submitted,

Timothy P. O'Hagan
Reg. No. 39,319

DATE: 5-13-08

Timothy P. O'Hagan
8710 Kilkenny Ct
Fort Myers, FL 33912
(239) 561-2300

24

Docket No.: Inno-024   *Marked to Show Changes*

1/9

Sub-Manager 20

Connection Module 24

Device State Machines 47

Active Connection Table 28

ID 46	Connection ID 48		Active Inactive 51	State Machine Address 49
	IP Address 50	Port 52		
Client 1				
Client 2				
Client 3				

Request State Machine 39

Message Handling 26

Trap Rules 38

Network Management Agent 25

Master MIB 32

	Value ID 210 (COID 188)	Value 1
MOID 1 182		
Client ID 46		
MOID 2		Value 2
MOID 3		Value 3

SNMP Manager 22

113

112   45

LAN 1 14a

FW 1 16a
Translation Table 17

IP Network 12

LAN 2 14b

FW 2 16b
Translation Table 17

10

Management Client 36a

Management Object 56a

Client 1 18a

MIB 34a	Value 1
COID 1	Value 1
COID 2	Value 2
COID 3	Value 3
188	44

Management Client 36b

Management Object 56b

Client 2 18b

MIB 34b	Value 1
COID 1	Value 1
COID 2	Value 2
COID 3	Value 3
188	44

Management Client 36c

Management Object 56c

Client 3 18c

MIB 34c	Value 1
COID 1	Value 1
COID 2	Value 2
COID 3	Value 3
188	44

Figure 1